

subscription identifier, and other information. See Applicants' specification, page 3, lines 24-27, and at least claims 1 (other information: e.g., a trusted mobile device identifier), claim 3 (a device identifier, and user agent information), and claims 4 and 7 (a gateway group identifier and a subscription identifier). Moreover, the server may also determine a level of trust based on whether the mobile device has defined operational capabilities, such as being enabled to accept a cookie or enabled to interact with a URL (see at least claim 1). Using such capability of the mobile device to select a level of trust and then determining at least one device signature based on that at least one level of trust is not taught or suggested by any of the cited prior art references.

For example, while Aura is cited for teaching multiple levels of authentication, Aura clearly fails to teach selecting such levels of authentication based on a capability of the mobile device. Instead, Aura teaches that “mobile node 202 may have achieved changing (e.g., decreasing or escalating) levels of authentication through multiple authentication operations during its interaction with the base station 200. Multiple authentication operations may occur, for example, as the mobile device 202 accesses different levels of services during its communications with the base station 200.” See Aura, Col. 7, lines 52-58. (Emphasis added). Thus, what Aura teaches is an approach that requires operations to be performed that, for example, includes accessing different levels of services, to obtain different levels of authentication. This is clearly very different from the Applicants’ claimed invention – which determines levels of trust **not based on performing accesses or other operations** – but, instead based on a capability or characteristic, in part, of the mobile device. Thus, determining a level of trust based on whether the mobile device is enabled to accept a cookie or enabled to interact with a URL is simply not taught or suggested by Aura.

Moreover, Jamtgaard also fails to teach or even suggest any such analysis is performed to determine if the mobile device is enabled to accept a cookie or interact with a URL to determine a trust level. In fact, Jamtgaard does not even teach testing for such capability of the mobile device. Instead, Jammtgaard discloses a content delivery system and method that allows different types of content be delivered to different information appliances having different protocols and different browser specifications. See Jammtgaard's Abstract. Jammtgaard is about not requiring re-

authoring of content information so that it can be displayed on each of the different devices. See Jammtgaard's Summary of the Invention, Col. 2, lines 40-59.

The Office Action cites Jammtgaard for teaching "if the mobile device is enabled to accept a cookie, then determining at least a second level of trust associated with the mobile device; and determining if the mobile device is enabled to interact with a URL, then determining at least a third level of trust associated with the mobile device." See page 4 of the pending Office Action. However, the Applicants respectfully submit that Jammtgaard does not teach or suggest this. Instead, Jammtgaard, at Column 5 merely mentions that "to intelligently harvest an HTML web page not only involves grabbing the content on the site (scraping), but also allows any functionality on that site to be enabled on the target information appliance or device. This enabled functionality may include, for example, forms, transactions, javascript, cookies, session data, and security measures. This enabled functionality is possible due to the virtual browser (See FIG. 7) that provides, for example, javascript and cookie proxy engines...." See Jammtgaard, Col. 5, lines 34-50. (Emphasis added). Thus, Jammtgaard merely mentions the word cookies, and does not make any mention of determining whether or not the mobile device (or target information appliance, using Jammtgaard's term) is enabled for accepting cookies – let alone determining a trust level based on such capability. The mere fact that Jammtgaard mentions a word that matches a search of words also found in the Applicants' claims is not sufficient to demonstrate that Jammtgaard teaches anything to do with the Applicants' claims.

Moreover, Jammtgaard also mentions the word "URL" at Col. 8, line 4 to Col 9, line 22. However, again, Jammtgaard does not make any determination of whether or not the mobile device is enabled to interact with a URL – let alone determining a trust level based on being enabled to interact with a URL. Instead, it appears that Jammtgaard assumes that it does, because, it expects to receive a request for page information of a particular URL website from the information appliance 15. See Jammtgaard, Col. 8, lines 7-9. Again, however, a mere usage of the same words as used in the Applicants' claims is not sufficient to teach or suggest the Applicants' claimed invention. Jammtgaard does not teach making a determination of whether or not the mobile device is capable of interacting with a URL. Furthermore, FIG. 7 of Jammtgaard teaches a virtual browser – but

Jammtgaard's virtual browser is not on the mobile device. Instead, the virtual browser is located on the translation server 12, and provides the important functionality of proxying javascript and cookies for the target devices. See Jammtgaard, Col. 10, lines 28-33. Thus, what Jammtgaard actually appears to teach instead is even if the mobile device does not have certain capabilities, those capabilities are provided for the mobile device so that it can access content from the content providers! Thus, Jammtgaard clearly appears to want each mobile device to get access to as much content as possible. Thus, Jammtgaard fails to teach or suggest the missing limitations of Aura.

Moreover, merely because Aura teaches multiple levels of authentication does not render the Applicants' claims obvious. Aura clearly teaches selection of such levels based on interactions with the mobile device as it accesses different levels of services. See above. This is not the same as determining levels of trust based on a capability of the mobile device as claimed in at least claim 1. Combining Jammtgaard with Aura clearly fails to fix Aura. As stated above, Aura appears to seek to limit access to content based on authentication; Jammtgaard provides a virtual browser that is not on the mobile device but is directed towards allowing access to different content. Thus, any combination of Jammtgaard with Aura would clearly change the principle operation of Aura. It remains valid that any such proposed modification or combination of the prior art that changes the principle operation of the prior art invention being modified is not sufficient to render the claims *prima facie* obvious. See MPEP §2143.01.VI.

In addition, because Jammtgaard fails to test or even suggest making a determination of whether or not the mobile device is capable of accepting a cookie or is enabled to interact with a URL, the conclusion must be that an artisan having common sense at the time of the invention would not have reasonably considered modifying Aura with Jammtgaard – which does not even teach or suggest such determinations as required by at least claim 1. This tenant remains true even after KSR. See, for example, *Ex Parte Green*, Appeal 20071271, decided June 12, 2007.

Independent Claims 18, 26, 35, 41, and 45 include similar, albeit different, features to independent Claim 1. For example, claims 35 and 41 recite, in part, determining if the mobile device is enabled with a defined operational capability and if the mobile device is so enabled, then

determining another level of trust associated with the mobile device. Claim 45 recites, in part, wherein at least one of the different levels of trust is based on an operational capability of the mobile device. Claims 18 and 26 further include limitations that include determining at least one level of trust based on whether the mobile device enabled to accept a cookie and/or interact with a URL. Thus, Applicants respectfully submit that, because the cited references do not support a *prima facie* rejection of at least the pending independent claims for at least the same reasons as stated above, the Applicants request that at least claims 1, 18, 26, 35, 41, and 45 be allowed to issue.

Regarding at least Claim 7, the Office Action submits that Laraki discloses determining a level of trust of a carrier associated with the mobile device based on at least one of a received subscription identifier and a gateway group identifier. However, the Applicants' submit that this is incorrect. Laraki does not teach or suggest such limitations. In fact, Laraki does not even teach at paragraphs 33-37 and 46-52 a subscription identifier or gateway group identifier at all! This again appears to be a misunderstanding based purely on a word search. What Laraki teaches at paragraph 0035 is a user identifier (UID). "The affiliated content provider of Laraki may use the UID information from the request to automatically authenticate the identity of the mobile user before delivering subscription content." As seen, the subscription refers to subscribing to access content based on the UID. This is made even clearer at paragraph 0036, where "if the mobile user is a subscriber, then the affiliated content provider 14 transmits the requested content to the wireless device 12 through the proxy server 22." However, as made clear in the Applicants' specification, the subscription identifier is not related to the mobile user, but is instead related to the mobile device. See for example, the Applicants' specification, page 7, lines 18-20, which says, "Carrier gateway 106 may be further configured to generate a subscription identifier based, in part, on the MIN number, and other information provided by mobile device 102 that may uniquely identifier [sic] mobile device 102." Thus, the subscription identifier used in at least claim 7 is clearly not the same subscription referred to in Laraki. They are unrelated at all. Therefore, Laraki's subscription to content can not render the Applicants' subscription identifier obvious. In fact, because they are so very different, there can be no teaching or suggestions by Laraki of at least claim 7. Therefore, the cited references simply do not render obvious at least claim 7 of the Applicants. Similarly,

because claims 4, 6, 10, 23, 28, 31, 36, and 42 each recite subscription identifiers, they too are also not rendered obvious by the cited references and therefore are also allowable for at least the same reason.

In addition, Claims 2-17 depend from Claim 1; Claims 19-25 depend from Claim 18; Claims 27-34 depend from Claim 26; Claims 36-40 depend from Claim 35; and Claims 42-44 depend from Claim 41. Therefore, for at least the same reasons as their respective independent claims, each of the dependent claims is also allowable. Thus, Applicant respectfully submits that Claims 1-45 are in condition for allowance, and should be allowed to issue.

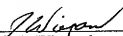
CONCLUSION

It is respectfully submitted that each of the presently pending claims (Claims 1-45) is in condition for allowance and notification to that effect is requested. Examiner is invited to contact the Applicants' representative at the below-listed telephone number if it is believed that the prosecution of this application may be assisted thereby. Although only certain arguments regarding patentability are set forth herein, there may be other arguments and reasons why the claimed invention is patentable. Applicant reserves the right to raise these arguments in the future.

In view of the above amendment, applicant believes the pending application is in condition for allowance.

Dated: February 20, 2008

Respectfully submitted,

By 
Jamie L. Wiegand
/ Registration No.: 52,361
DARBY & DARBY P.C.
P.O. Box 770
Church Street Station
New York, New York 10008-0770
(206) 262-8915 / (212) 527-7701 (Fax)
Attorneys/Agents For Applicant